What is claimed is:

1. A security management system for controlling a
security status of each of a plurality of managed
systems constituting an information system in
accordance with an information security policy
representing a policy of a security measure,
comprising:

a plurality of management sections corresponding
to at least one managed system and the information
security policy, each management section being for
controlling the security status of the managed system
corresponding thereto so as to adjust the security
status to the information security policy
corresponding thereto;

a database registering a correspondence of the
information security policy, the managed system and
each management section;

a security content reception section for
receiving a selection of a range of the information
security policy and the managed system from a user;

an extraction section for extracting from said
database the management section registered so as to
correspond to the information security policy and the

23 managed system included in the range in which said

24 security content reception section has received the

25 selection; and

26   a management control section for allowing the

27 management section extracted by said extraction

28 section to change the security status of the managed

29 system corresponding to the management section so as

30 to adjust to the information security policy corre-

31 sponding to the management section.

1 2. A security management system for auditing a security

2 status of each of a plurality of managed systems

3 constituting an information system, the security

4 status concerning an information security policy

5 representing a policy of a security measure,

6 comprising:

7   a plurality of audit sections corresponding to

8 at least one managed system and at least one

9 information security policy, each audit section being

10 for auditing the security status concerning the

11 corresponding information security policy of the

12 corresponding managed system;

13   a database registering a correspondence of the

14 information security policy, the managed system and

15 the audit section;

16   a security content reception section for

17 receiving a selection of a range of the information

18 security policy and the managed system from the user;

19 an extraction section for extracting from said

20 database the audit section registered so as to

21 correspond to the information security policy and the

22 managed system included in the range in which said

23 security content reception section has received the

24 selection; and

25 an audit control section for allowing the audit

26 section extracted by said extraction section to audit

27 the security status concerning the information

28 security policy of the managed system corresponding

29 to the audit section.

1 3. A security management system for controlling a

2 security status of each of a plurality of managed

3 systems constituting an information system in

4 accordance with an information security policy

5 representing a policy of a security measure,

6 comprising:

7 a plurality of management sections corresponding

8 to at least one managed system and at least one

9 information security policy, each management section

10 being for controlling the security status of the

11 corresponding managed system so as to adjust the

12 security state to the corresponding information

13   security policy;

14   a plurality of audit sections corresponding to

15   at least one managed system and at least one

16   information security policy, each audit section being

17   for auditing the security status concerning the

18   corresponding information security policy of the

19   corresponding managed system;

20   a database registering a correspondence of the

21   information security policy, the managed system, the

22   management section and the audit section;

23   a security content reception section for

24   receiving a selection of a range of the information

25   security policy and the managed system from a user;

26   an extraction section for extracting from said

27   database the management section and the audit section,

28   which are registered so as to correspond to the

29   information security policy and the managed system

30   included in the range in which said security content

31   reception section has received the selection;

32   a management control section for allowing the

33   management section extracted by said extraction

34   section to change the security status of the managed

35   system corresponding to the management section so as

36   to adjust to the information security policy corre-

37   sponding to the management section; and

38   an audit control section for allowing the audit

39 section extracted by said extraction section to audit

40 the security status concerning the information

41 security policy of the managed system corresponding

42 to said audit section.

1 4. A security management method for controlling a

2 security status of each of a plurality of managed

3 systems constituting an information system with an

4 electronic computer in accordance with an information

5 security policy representing a policy of a security

6 measure, comprising the steps of:

7 receiving a selection of a range of the

8 information security policy and the managed system

9 from a user;

10 extracting a management program corresponding to

11 an information security policy and a managed system,

12 included in the range in which the selection has been

13 received, among a plurality of management programs

14 describing a processing for controlling the security

15 status of the corresponding managed system so as to

16 adjust the security status to the corresponding

17 information security policy, the plurality of

18 management programs corresponding to at least one

19 information security policy and at least one managed

20 system, which are previously stored; and

21 allowing the electronic computer to execute the

22 extracted management program and to change the

23 security status of the managed system corresponding

24 to the management program so that the security status

25 thereof is adjusted to the information security policy

26 corresponding to the management program.

1 5. A security management method for auditing, with an

2 electronic computer, a security status of each of a

3 plurality of managed systems constituting an

4 information system, the security status concerning an

5 information security policy representing a policy of

6 a security measure, comprising the steps of:

7   receiving a range of a selection of the

8 information security policy and the managed system

9 from a user;

10   extracting an audit program registered so as to

11 correspond to the information security policy and the

12 managed system, which are included in the range in

13 which the selection has been received, among a

14 plurality of audit programs describing a processing

15 for auditing the security status concerning the

16 corresponding information security policy of the

17 corresponding managed system, the plurality of audit

18 programs corresponding to at least one information

19 security policy and at least one managed system, which

20 are previously stored; and

54

21   allowing the electronic computer to execute the

22   extracted audit program and to audit the security

23   status of the managed system corresponding to the audit

24   program, the security status concerning the

25   information security policy corresponding to the audit

26   program.

1   6. A storage medium storing a program for controlling

2   a security status of each of a plurality of managed

3   systems constituting an information system in

4   accordance with an information security policy

5   representing a policy of a security measure,

6   wherein said program is read out and executed by

7   an electronic computer,

8   to construct, on said electronic computer,

9   a security content reception section for

10   receiving a selection of a range of the information

11   security policy and the managed system from a user;

12   an extraction section for extracting a management

13   program corresponding to an information security

14   policy and a managed system, which are included in the

15   range in which said security content reception section

16   has received the selection, from a database storing

17   a plurality of management programs describing a

18   processing for controlling the security status of the

19   corresponding managed system so as to adjust the

20 security status of the managed system to the corre-

21 sponding information security policy, the plurality

22 of management programs corresponding at least one

23 managed system and at least one information security

24 policy; and

25   a management control section for allowing said

26 electronic computer to execute the management program

27 executed by said extraction section and to change the

28 security status of the managed system corresponding

29 to the extracted management program so as to adjust

30 the security status to the information security policy

31 corresponding to the extracted management program.

1 7. A storage medium storing a program for auditing a

2 security status concerning an information security

3 policy representing a policy of a security measure of

4 a plurality of managed systems constituting an

5 information system,

6   wherein said program is read out and executed by

7 an electronic computer,

8   to construct, on said electronic computer,

9   a security content reception section for

10 receiving a selection of a range of the information

11 security policy and the managed system from a user;

12   an extraction section for extracting an audit

13 program registered so as to correspond to an

14 information security policy and a managed system,

15 which are included in the range in which said security

16 content reception section has received the selection,

17 from a database storing a plurality of audit programs

18 describing a processing for auditing the security

19 status concerning the corresponding information

20 security policy of the corresponding managed system,

21 the plurality of audit programs corresponding to at

22 least one managed system and at least one information

23 security policy; and

24   an audit control section for allowing the

25 electronic computer to execute the audit program

26 extracted by said extraction section and to audit the

27 security status concerning the information security

28 policy corresponding to the audit program of the

29 managed system corresponding to the audit program.

1 8. A security management method for supporting a

2 security management of each of a plurality of managed

3 systems constituting an information system with an

4 electronic computer, comprising:

5   a security specification hatching step of ex-

6 tracting an information security policy made to

7 correspond to each managed system constituting an

8 information system designated by a user from a database

9 describing a correspondence of an information security

10   policy representing a policy of a security measure with

11   at least one managed system, to hatch security

12   specifications to be applied to the information

13   system;

14   a security diagnosis step of executing a

15   plurality of audit programs describing a processing

16   for auditing various information including a type of

17   the managed system and a software version, which are

18   stored so as to correspond to each set of the

19   information security policy and the managed system,

20   the information security policy and the managed system

21   being specified by security specifications hatched in

22   said security specification hatching step, as well as

23   a security status concerning the information security

24   policy of the managed system, to audit the various

25   information including the type and the software

26   version of the managed system constituting the

27   information system designated by the user, and to

28   diagnose a security of said information system; and

29   a security handling and management step of ex-

30   ecuting a management program designated by the user,

31   among a plurality of management programs describing

32   a processing for controlling the security status

33   concerning the information security policy of the

34   managed system stored so as to correspond to each set

35   of the information security policy and the managed

58

36 system, which are specified by the security

37 specifications hatched in said security specification

38 hatching steps, to allow said electronic computer to

39 change the security status of the managed system

40 corresponding to the management program so as to adjust

41 the security status to the information security policy

42 corresponding to the management program.

1 9. The security management method according to claim

2 8,

3 wherein, in said security diagnosis step, the

4 audit program made to correspond to each set of the

5 information security policy and the managed system,

6 which are specified by the security specifications

7 hatched in said security specification hatching step,

8 is extracted from a database describing a

9 correspondence of the information security policy, the

10 managed system and the audit program describing a

11 processing for auditing various information such as

12 a type and a software version of said managed system

13 as well as the security status concerning said

14 information security policy of said managed system,

15 and executed, to diagnose the security of the

16 information system designated by said user; and

17 in said security handling and management step,

18 the management programs made to correspond to each set

19 of the information security policy and the managed
20 system, which are specified by the security
21 specifications hatched in said security specification
22 hatching step, are extracted from a database
23 describing a correspondence of the information
24 security policy, the managed system and the management
25 program describing a processing for controlling the
26 security status concerning the security policy, the
27 managed system and said information security policy
28 of a security of said managed system, and the
29 management program designated by the user is extracted
30 among the extracted programs to be executed, to allow
31 the security status of the managed system
32 corresponding to the extracted management program to
33 adjust to the information security policy
34 corresponding to the management program.

1 10. The security management method according to claim
2 8,
3   wherein said security diagnose step is executed
4 periodically.

1 11. The security management method according to claim
2 8,
3   wherein, in accordance with a setting content
4 received from the user, said management program

5   changes the security status of the managed system

6   corresponding to the management program so as to adjust

7   the security status to the information security policy

8   corresponding to the management program.

1   12. The security management method according to claim

2   8,

3   wherein a security hole information published by

4   a security information organization including CERT or

5   Computer Emergency Response Team and diagnosis results

6   obtained in said security diagnose step which is

7   executed for the information system designated by the

8   user are reflected in the database describing the

9   correspondence of the information security policy with

10 at least one managed system and an audit/management

11 program stored so as to correspond to each set of the

12 information security policy and the managed system.

1   13. A security management system for supporting a

2   security management of managed systems constituting

3   an information system, comprising:

4   a database describing a correspondence of an

5   information security policy representing a policy of

6   a security measure with at least one managed system;

7   a security specification hatching section for

8   extracting an information security policy made to

9   correspond to each of the managed systems constituting

10   the information system designated by a user from said

11   database, to hatch security specifications to be

12   applied to the information system;

13   a plurality of audit sections for auditing

14   various information including a type and a software

15   version of the managed system as well as a security

16   status concerning the information security policy of

17   the managed system, each audit section being provided

18   so as to correspond to each set of the information

19   security policy and the managed system, which are

20   specified by security specifications hatched by said

21   security specification hatching section, and;

22   a security diagnosis section for diagnosing a

23   security of an information system designated by said

24   user, on the basis of diagnosis results in each of said

25   audit sections;

26   a plurality of management sections for

27   controlling a security status concerning the

28   information security policy of the managed system,

29   each management section being provided so as to

30   correspond to each set of the information security

31   policy and the managed system, which are specified by

32   security specifications hatched by said security

33   specification hatching step, and;

34   a security handling and management section for

35   executing a management section designated by said user,

36   to change the security status of the managed system

37   corresponding to the management program so as to adjust

38   the security status to the information security policy

39   corresponding to the management program.